Application No.: 09/872,077
Amendment Dated 04/12/2006
Reply to Office Action of 01/12/2006

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A computer system for encrypting and decrypting a data element using a static key and a dynamic key, comprising:
said data element being statically encrypted with said static key;
an encryption state being associated with said data element being statically encrypted with said static key;
said data element being dynamically encrypted with said dynamic key; and
said data element being decrypted with said dynamic key and said static key on a receiving computer system, wherein in response to a transmission failure of a previous~~said~~ data element, ~~decryption of~~ said data element also being decrypted with said encryption state, ~~recovered~~ without retransmission of said previous data element.

2. (original) The computer system of Claim 1, wherein encryption with said static key is strong encryption.

3. (original) The computer system of Claim 1, wherein encryption with said dynamic key is weak encryption.

4. (previously presented) The computer system of Claim 1, wherein:
said data element is encrypted with said static key on a first computer system;
said data element is encrypted with said dynamic key on a second computer system; and
thereby encryption and decryption are distributed between said first computer system, said second computer system, and said receiving computer system.

5. (original) The computer system of Claim 4, wherein said second computer system is untrusted.

6. (previously presented) The computer system of Claim 1, wherein:

said data element is encrypted with said static key on a first computer system;
said data element is encrypted with said dynamic key on said first computer system; and
thereby encryption and decryption are distributed between said first computer system and said receiving computer system.

7. (currently amended) A computer implemented method for encrypting a data element and decrypting said data element using a static key and a dynamic key, comprising:
encrypting said data element with said static key, wherein said encrypting maintains an encryption state;
encrypting said data element with said dynamic key;
transmitting said encrypted data element with said encryption state to a receiving computer system;
decrypting said encrypted data element with said static key and said dynamic key on said receiving computer system; and
determining when transmission of ~~said~~ a previous encrypted data element failed; and
in response to said determining said transmission of said previous encrypted data element failed, ~~recovering said~~ decrypting ~~of~~ said encrypted data element with said static key, said encryption state and said dynamic key without retransmission of said previous encrypted data element.

8. (previously presented) The method of Claim 7, said encrypting said data element with said static key strongly encrypts said data element with said static key.

9. (previously presented) The method of Claim 7, wherein said encrypting said data element with said dynamic key weakly encrypts said data element with said dynamic key.

10. (previously presented) The method of Claim 7, further comprising:
wherein said encrypting said data element with said static key is on a first computer system;
transmitting said data element to a second computer system;
wherein said encrypting said data element with said dynamic key is on said second computer system; and

thereby distributing encryption and decryption between said first computer system, said second computer system, and said receiving computer system.

11. (previously presented) The method of Claim 7,
wherein said encrypting said data element with said static key is on a first computer system;
wherein said encrypting said data element with said dynamic key is on said first computer system; and
thereby distributing encryption and decryption between said first computer system and said receiving computer system.

12. (currently amended) The method of Claim 7[[10]], wherein said transmitting transmits a value of said encryption state that is prior to said encrypting of said data element with said static key~~further comprising:~~
~~determining when transmission of said data element from said first computer system to said second computer system failed; and~~
~~recovering said decrypting of said data element without retransmission of said data~~.

13. (canceled)

14. (canceled)

15. (currently amended) An article of manufacture comprising a program storage medium readable by a computer and embodying one or more instructions executable by the computer for causing a computer system to encrypt a data element and decrypt said data element using a static key and a dynamic key, comprising:
encrypting said data element with said static key, wherein said encrypting maintains an encryption state;
encrypting said data element with said dynamic key;
transmitting said encrypted data element with said encryption state to a receiving computer system;

decrypting said encrypted data element with said static key and said dynamic key on said receiving computer system;

determining when transmission of ~~said~~ a previous encrypted data element failed; and

in response to said determining said transmission of said previous encrypted data element failed, ~~recovering said~~ decrypting ~~of~~ said encrypted data element with said static key, said encryption state and said dynamic key without retransmission of said previous encrypted data element.

16. (previously presented) The article of manufacture of Claim 15 wherein said encrypting said data element with said static key strongly encrypts said data element with said static key.

17. (previously presented) The article of manufacture of Claim 15 wherein said encrypting said data element with said dynamic key weakly encrypts said data element with said dynamic key.

18. (previously presented) The article of manufacture of Claim 15, further comprising:

wherein said encrypting said data element with said static key is on a first computer system;

transmitting said data element to a second computer system;

wherein said encrypting said data element with said dynamic key is on said second computer system; and

thereby distributing encryption and decryption between said first computer system, said second computer system, and said receiving computer system.

19. (previously presented) The article of manufacture of Claim 15,

wherein said encrypting said data element with said static key is on a first computer system;

wherein said encrypting said data element with said dynamic key is on said first computer system; and

thereby distributing encryption and decryption between said first computer system and said receiving computer system.

20. (currently amended) The article of manufacture of Claim 15[[18]], wherein said encrypting said data element with said static key uses said encryption state to vary values of said data element encrypted with static key~~further comprising:~~

~~determining when transmission of said data element from said first computer system to said second computer system failed; and~~

~~recovering said decrypting of said data element without retransmission of said data~~.

21. (canceled)

22. (canceled)

23. (currently amended) A computer system for encrypting and decrypting a data element using a static key and a dynamic key, said data element being partitioned into a plurality of chunks, comprising:

said data element chunks being statically encrypted with said static key;

encryption states being associated with said data element chunks being statically encrypted with said static key;

said data element chunks being dynamically encrypted with said dynamic key; and

said data element chunks being decrypted with said dynamic key and said static key on a receiving computer system, wherein in response to a transmission failure of a previous one of said data element chunks, a subsequent one of said data element chunks being decrypted with said static key, one of said encryption states, and said dynamic key ~~decryption of said data element chunks being recovered~~ without retransmission of said previous one of said data element chunks.

24. (original) The computer system of Claim 23 wherein encryption with said static key is strong encryption.

25. (original) The computer system of Claim 23, wherein encryption with said dynamic key is weak encryption.

26. (previously presented) The computer system of Claim 23, wherein:

said data element chunks are encrypted with said static key on a first computer system;

said data element chunks are encrypted with said dynamic key on a second computer system; and

thereby encryption and decryption are distributed between said first computer system, said second computer system, and said receiving computer system.

27. (original) The computer system of Claim 26, wherein said second computer system is untrusted.

28. (previously presented) The computer system of Claim 23, wherein:
said data element chunks are encrypted with said static key on a first computer system;
said data element chunks are encrypted with said dynamic key on said first computer system; and
thereby encryption and decryption are distributed between said first computer system and said receiving computer system.

29. (currently amended) A computer implemented method for encrypting a data element and decrypting said data element using a static key and a dynamic key, said data element being partitioned into chunks, comprising:
encrypting said data element chunks with said static key to provide static encrypted data element chunks, said static encrypted data element chunks being associated with static encryption states, respectively, said static encryption states being used to vary values of said static encrypted data element chunks being statically encrypted with said static key;
encrypting said static encrypted data element chunks with said dynamic key to provide dynamic-static data element chunks ~~and dynamic encryption recovery information states~~;
transmitting said dynamic-static data element chunks and said ~~dynamic~~ static encryption ~~information~~ states to a receiving computer system;
decrypting said dynamic-static data element chunks with said static key and said dynamic key on said receiving computer system;
determining, on said receiving computer system, when transmission of a previous one of said dynamic-static data element chunks failed; and
in response to said determining said transmission of said previous one of said dynamic-static data element chunks failed, decrypting a subsequent one of said dynamic-static data element chunks with said static key, said dynamic key and said static encryption state, wherein said previous one of said dynamic-static data element chunks associated with said failed transmission is not

recoveredrecovering, on said receiving computer system, said decrypting of said dynamic-static data element chunks after said one of said dynamic-static data element chunks based on one of said dynamic encryption recovery information states.

30. (previously presented) The method of Claim 29 wherein said encrypting said data element chunks with said static key strongly encrypts said data element chunks with said static key.

31. (previously presented) The method of Claim 29 wherein said encrypting said static encrypted data element chunks with said dynamic key weakly encrypts said data element chunks with said dynamic key.

32. (previously presented) The method of Claim 29, further comprising:
wherein said encrypting said data element chunks with said static key is on a first computer system;
transmitting said static encrypted data element chunks to a second computer system;
wherein said encrypting said static encrypted data element chunks with said dynamic key is on said second computer system; and
thereby distributing encryption between said first computer system and, said second computer system.

33. (previously presented) The method of Claim 29,
wherein said encrypting said data element chunks with said static key is on a first computer system;
wherein said encrypting said static encrypted data element chunks with said dynamic key is on said first computer system.

34. (currently amended) The method of Claim 29[[32]], wherein said previous one of said dynamic-static data element chunks associated with said failed transmission is not retransmittedfurther comprising:
transmitting said static encrypted data element chunks with static encryption recovery information;

~~determining when transmission of said static encrypted data element chunks from said first computer system to said second computer system failed; and~~

~~recovering said decrypting of at least one of said data element chunks without retransmission of said data based on said static encryption recovery information.~~

35. (canceled)

36. (canceled)

37. (currently amended) An article of manufacture comprising a program storage medium readable by a computer and embodying one or more instructions executable by the computer for causing a computer system to encrypt a data element and decrypt said data element using a static key and a dynamic key, said data element being partitioned into chunks, comprising:

encrypting said data element chunks with said static key, wherein said encrypting maintains an encryption state;

encrypting said data element chunks with said dynamic key;

transmitting said data element chunks with said encryption state to a receiving computer system;

decrypting said data element chunks with said static key and said dynamic key on said receiving computer system;

determining when transmission of said data element chunks from said second computer system to said receiving computer system failed; and

in response to said determining said transmission of said one of said dynamic-static data element chunks failed, ~~recovering said~~ decrypting ~~of~~ a subsequent one of said data element chunks with said static key, said encryption state and said dynamic key without retransmission of said one of said dynamic-static data element chunks associated with said failed transmission.

38. (previously presented) The article of manufacture of Claim 37 wherein said encrypting said data element chunks said static key weakly encrypts said data element chunks with said static key.

39. (previously presented) The article of manufacture of Claim 37 wherein said encrypting said data element chunks with said dynamic key weakly encrypts said data element chunks with said dynamic key.

40. (previously presented) The article of manufacture of Claim 37, further comprising:
wherein said encrypting said data element chunks with said static key is on a first computer system;
transmitting said data element chunks to a second computer system;
wherein said encrypting said data element chunks with said dynamic key is on said second computer system; and
thereby distributing encryption between said first computer system and said second computer system.

41. (previously presented) The article of manufacture of Claim 37,
wherein said encrypting said data element chunks with said static key is on a first computer system;
wherein said encrypting said data element chunks with said dynamic key is on said first computer system.

42. (previously presented) The article of manufacture of Claim 40, further comprising:
determining when transmission of said data element chunks from said first computer system to said second computer system failed; and
recovering said decrypting of said data element chunks without retransmission of said data.

43. (canceled)

44. (canceled)